

REMARKS

This Application has been carefully reviewed in light of the *Office Action*. At the time of the *Office Action*, Claims 1-26, and 30-35 were pending and rejected. Applicant has amended Claims 5, 9-10, 14, 16-23, and 30-31 and canceled Claim 32. Applicant respectfully requests reconsideration and favorable action in this case.

Rejections Under 35 U.S.C. § 112

The Examiner rejected Claims 9, 10, 14, 17-23, 31, and 32 under U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Applicant has amended Claims 9-10, 14, 16-23, and 31 in a fashion which renders the § 112 rejections of those claims moot. Applicant has also canceled Claim 32, rendering the § 112 rejection of that claim moot.

Rejections Under 35 U.S.C. §103

The Examiner, under 35 U.S.C. § 103(a), rejected as allegedly being unpatentable: Claims 1-5, 9-11, 15-20, 24-26, 30-32, 34, and 35 over U.S. Publication No. 2003/0061515 by Kindberg et al. ("*Kindberg*") in view of U.S. Patent No. 7,231,666 to Haugh ("*Haugh*") and U.S. Publication No. 2005/0050353 by Thiele et al. ("*Thiele*"); Claims 6-8, 12-14, and 21-23 over *Kindberg* in view of *Haugh* and *Thiele* and further in view of U.S. Patent No. 7,080,000 to Cambridge ("*Cambridge*"); and Claim 33 over *Kindberg* in view of *Haugh* and *Thiele* and further in view of U.S. Patent No. 6,968,394 to El-Rafie ("*El-Rafie*"). Applicant respectfully traverses those rejections for the reasons stated below.

- I. There is no motivation to combine *Kindberg* with *Haugh* as proposed by the Examiner because the proposed combination would change *Kindberg's* principle of operation.**

Claim 1 is directed to a method for maintaining computer security. As such, Claim 1 includes the limitations:

at a reverse proxy server residing between at least one client computer and a web server: . . .

comparing a length of a URL in a message header of the incoming message ("the incoming URL") with the predefined length in the signature file to determine whether the incoming message is malicious; and

if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server.

To reject those limitations, the Examiner relies on a combination of *Kindberg* and *Haugh*. In particular, the *Office Action* states that although *Kindberg* does not,

explicitly disclose . . . comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file and if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server[.]. . . . *Haugh* discloses . . . comparing a length of an argument with the predefined length in the signature file and if the length exceeds the predefined length (*[i.e.,] if the length of the command line argument being processed exceeds a hard limit*), blocking the argument [column 5, lines 50-55 & Figure 5].

See *Office Action*, page 4 line 15 - page 5 line 6 (emphasis original). The Examiner then argues that it would have been obvious to combine *Kindberg* with *Haugh* “in order to facilitate the identification and prevention of buffer overflow attacks. . . .” See *Office Action*, page 5 lines 10-13. Applicant respectfully disagrees.

Without conceding that the Examiner’s proposed modification is technically feasible or that the Examiner’s descriptions of the references are technically accurate, even if it were possible to modify the references as the Examiner suggests such that *Kindberg*’s invention identified and prevented buffer overflow attacks, that modification would completely change *Kindberg*’s principle of operation.

As explained in Applicant’s previous response dated June 1, 2009 (the “*Previous Response*”), *Kindberg* is directed to “[a] mechanism for providing a user with selective access to resources on an intranet.” See *Kindberg*, Abstract. As further explained by *Kindberg*,

[r]equests for access to resources inside the intranet are made through the reverse proxy server. Access to the requested resource is provided to the client by means of a capability-enabled uniform resource locator (URL) having a character string that is produce by encoding an identification number and a random number. ***The character string, identification number and random number are associated with a database record accessed by the reverse proxy server to determine whether access is to be provided to the client, and what conditions to apply to the access*** when the capability-enabled URL is invoked.

See *id.* (emphasis added). That is, *Kindberg* discloses that its invention operates by associating an “identification number” and a “random number” (included as part of a URL)

with a database record in order to determine whether to provide a client with access to a requested resource. However, the Examiner's rejection completely changes that principle of operation.

In particular, the Examiner's proposed modification would change the alleged selective access system of *Kindberg* from a system designed to "determine whether access is to be provided to the client" based on whether a "character string, identification number and random number are associated with a database record;" see *Kindberg*, Abstract, to a system that inhibits access to a resource based on whether "*the length of the command line argument being processed exceeds a hard limit.*" See *Office Action*, page 5 lines 3-6 (emphasis original).

The MPEP explicitly states that there is no motivation to combine references under this set of facts. "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are *not sufficient* to render the claims *prima facie* obvious." MPEP §2143.01 (emphasis added). Additionally, the examination guidelines issued by the United States Patent and Trademark Office ("PTO") in response to the U.S. Supreme Court's recent decision in *KSR Int'l Co. v. Teleflex, Inc.* state, in part, that "[t]he rationale to support a conclusion that the claim would have been obvious is that all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods *with no change in their respective functions....*" *Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in KSR International Co. v. Teleflex Inc.*, 72 Fed. Reg. 57526, 57529 (Oct. 10, 2007) (emphasis added).

According to this legal principle, Applicant respectfully contends that the Examiner's proposed combination of *Kindberg* with *Haugh* is improper and that Claim 1 and each of its dependent claims (e.g., Claims 2-8, 30, 33, and 36) are in condition for allowance. For analogous reasons, Applicants further contend that Claims 9, 16 and 34 and each of their respective dependent claims (e.g., Claims 10-15 and 31, Claim 17-26, and Claim 35) are in condition for allowance.

II. No cited reference shows the combination of limitations recited in Claim 30.

Claim 30 is directed to the method of Claim 1:

wherein the information comprises a list of known system vulnerabilities; and further comprising:

comparing one or more characteristics of the incoming message with the list to determine whether the incoming message is malicious ; and

if the one or more characteristics *fail to satisfy* any of the vulnerabilities on the list of known system vulnerabilities, determining that the incoming message is not malicious and forwarding the incoming message to the web server.

No reference shows this combination of limitations. For example, the Examiner relies on a capability verification procedure described in paragraph [0054] of *Kindberg's* to teach the step of "comparing the received incoming message with the signature file to determine whether the incoming message is malicious (*ie. step 610*).” See *Office Action*, page 4, lines 11-12. However, that passage discloses that the invention of *Kindberg* relies on *successfully matching* the alleged incoming URL to a record in a database. According to paragraph [0054]:

In step 610, the capability is verified by first determining whether the resolved identification number corresponds to a database record. If a database record exists for the identification number, the decoded expected random number is checked for a match with the random number in the identified database record. **If a record exists for the decoded identification number and the random number in the record matches the expected random number, then the capability is accepted as genuine. If either the identification number or random number does not match, the request is rejected and can either be ignored or responded to with an error message.**

Kindberg, paragraph [0054] (emphasis added). That is, this paragraph discloses that alleged request is *rejected* if either the identification number or random number does not match. By contrast, Claim 30 recites “if the one or more characteristics fail to satisfy any of the vulnerabilities on the list of known system vulnerabilities, *determining that the incoming message is not malicious and forwarding the incoming message to the web server.*” For at least those reasons, Applicant respectfully contends Claim 30 is in condition for allowance.

III. No cited reference shows a list including at least one known system vulnerability specific to the web server as recited in Claim 31.

Claim 31 is directed to the method of Claim 1:

wherein the information comprises a list of known system vulnerabilities *specific to* the web server, and further comprising:

comparing one or more characteristics of the incoming message with the list to determine whether the incoming message is malicious ; and

if the one or more characteristics fail to satisfy any of the vulnerabilities on the list of known system vulnerabilities, determining that the incoming message is not malicious and forwarding the incoming message to the web server.

No reference shows this combination of limitations. For example, the Examiner relies on *Kindberg's* list of acceptable arguments for CGI scripts to teach the known system vulnerabilities of Claim 31. However, *Kindberg* is devoid of any teaching that those acceptable arguments are specific to any component of *Kindberg*. For at least those reasons, Applicant respectfully contends Claim 31 is in condition for allowance.

IV. All Claims are in condition for allowance.

For at least the reasons stated above, Applicant respectfully contends that each and every claim is in condition for allowance. Moreover, Applicant respectfully contends that none of the deficiencies described above with respect to *Kindberg* are accounted for by any of the remaining references cited by the Examiner or by the knowledge of one of ordinary skill in the art.

V. No Waiver

Additionally, Applicant has merely discussed example distinctions from the references cited by the Examiner. Other distinctions may exist, and Applicant reserves the right to discuss these additional distinctions in a later Response or on Appeal, if appropriate. By not responding to additional statements made by the Examiner, Applicant does not acquiesce to the Examiner's additional statements, nor does Applicant necessarily concede to the veracity of any characterization of Applicant's claims or the prior art references made by the Examiner. The example distinctions discussed by Applicant are sufficient to overcome the Examiner's rejections.

CONCLUSION

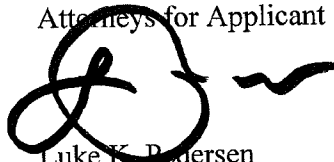
Applicant has made an earnest attempt to place this case in condition for allowance. For at least the foregoing reasons, Applicant respectfully requests full allowance of all the pending claims.

If the Examiner believes a telephone conference would advance prosecution of this case in any way, the Examiner is invited to contact Luke K. Pedersen, the Attorney for Applicant, at the Examiner's convenience at (214) 953-6655.

Applicant believes no fee is due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to **Deposit Account No. 02-0384 of BAKER BOTTS L.L.P.**

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant



Luke K. Pedersen
Reg. No. 45,003

Date: November 19, 2009

CORRESPONDENCE ADDRESS:

Customer No. **05073**